REMARKS

Claims 1, 2, 5-13 and 16-25 were previously pending. No claims are amended, added or canceled. Claims 1, 2, 5-13 and 16-25 remain pending.

35 U.S.C. § 102 Rejections

Claims 1, 2, 5-13 and 16-25 stand rejected under 35 U.S.C. 102 as being anticipated by U.S. Patent No. RE 36,946 to Diffie, et al. (hereinafter "Diffie"). Applicant respectfully traverses the rejection.

Diffie discloses a method and apparatus for providing a secure network communication link between a mobile computer and a base computer. The mobile sends a host certificate to the base with a random number and list of shared key algorithms. **The certificate is digitally signed by a trusted certification authority.** If the certificate is not valid, the base rejects the connection attempt. The base then sends a certification, random number and identifier to the mobile. The base signs the message and sends it to the mobile.

The mobile validates the base certificate and, if valid, verifies the base signature with a base public key. If the base signature is invalid, then the communication attempt is aborted. If the base signature is valid, the mobile generates and sends an encrypted message that includes a session key to the base after signing the message with the mobile's private key.

The base verifies the mobile signature using a mobile public key. If the signature is valid, the base decrypts the message using a base private key to determine the session key. The mobile and base then enter a data transfer phase using encrypted data which is decrypted using the session key.

Claim 1

Claim 1 recites a method for "a mobile computing device to make authentication information available to a base computing device." The method includes a step of creating authentication information that includes:

"content data that include data for updating a care-of address of the mobile computing device";

"a public key of the mobile computing device";

"a network address of the mobile computing device ... having a portion derived from the public key of the mobile computing device;"

"a digital signature generated by signing with a private key of the mobile computing device corresponding to the public key;" and

"the digital signature generated from "content data" and/or "a hash value of data including the content data."

The authentication information is made available to the base computing device.

To support a rejection under Section 102, the cited reference(s) must include each and every element of the rejected claim. In this instance, Diffie does not disclose or anticipate each and every element of claim 1.

Claim 1 requires that the mobile computing unit create and send authentication information to the base computing unit. The authentication information must include, *inter alia*, "a network address of the mobile computing device ... having a portion derived from the public key of the mobile computing device." Diffie does not disclose or anticipate an authentication message that includes such information. In fact, Diffie does not disclose or anticipate any kind of derivation of a network address using any data, let alone a public key of the mobile computing device.

Claim 1 also recites that content data sent from the mobile to the base include "data for updating a care-of address of the mobile computing device."

Diffie does not disclose or anticipate this element of claim 1. In this context, the "care-of address" refers to an address to which, *inter alia*, a home agent forwards data originating from a correspondent. In other words, the care-of address implies the use of at least three logical network devices: the correspondent, the home agent, and the device having the care-of address. The topology in Diffie discusses only two logical network devices and does not discuss forwarding data between any network devices.

The method of claim 1 allows the base computing unit to unilaterally verify a network address of the mobile unit when the mobile unit updates an address to which messages received at the base computing unit can be forwarded to the mobile computing unit. Claim 1 describes a lightweight protocol that can be used as the mobile computing unit roams between different networks. The lightweight protocol is not as burdensome as the method disclosed by Diffie, which requires many different steps to authenticate a connection.

Diffie does not disclose or anticipate the method recited in claim 1. Accordingly, claim 1 is allowable over the cited reference and the rejection of claim 1 should be withdrawn.

Claims 2 and 5-11

Claims 2 and 5-11 depend from claim 1 and are allowable at least by virtue of that dependency. Accordingly, the rejection of these claims should be withdrawn.

Claims 3 and 4

Claims 3 and 4 have been canceled, thereby rendering the rejection thereof moot.

Claim 12

Claim 12 recites a computer-readable having instructions performing a method of "creating authentication information, the authentication information including content data that include data for updating a care-of address of the first

computing device, a public key of the first computing device, a network address of the first computing device, and a digital signature, the network address having a portion derived from the public key of the first computing device, the digital signature generated by signing with a private key of the first computing device corresponding to the public key, the digital signature generated from data in the set: the content data, a hash value of data including the content data."

Claim 12 is similar to claim 1 in that claim 12 requires that a mobile computing device create authentication information that includes, *inter alia*, a network address having a portion derived from a public key of the first computing device. By the same rationale recited in the response to the rejection of claim1, at least this element is neither disclosed not anticipated by Diffie.

Accordingly, claim 12 is allowable over the cited reference and the rejection thereof should be withdrawn.

Claim 13

Claim 13, recites a computer-readable medium containing a data structure that comprises: (1) "content data that include data for updating a care-of address of a computing device" (2) "a public key of the computing device" (3) "a network address of the computing device, the network address having a portion derived from the public key of the computing device" and (4) "a digital signature, the digital signature generated by signing with a private key of the computing device corresponding to the public key, the digital signature generated from data in the set: the content data, a hash value of data including the content data."

Diffie does not disclose at least elements (1) and (3). Diffie does not disclose or anticipate anything regarding a care-of address of a computing device. Neither does Diffie disclose deriving a network address using a public key of the computing device. As such, Diffie does not disclose or anticipate each and every element of claim 13 as required to support a Section 102 rejection.

Accordingly, claim 13 is allowable over the cited rejection and the rejection should be withdrawn.

Claims 14 and 15

Claims 14 and 15 have been canceled thereby rendering the rejection thereof moot.

Claims 16-19

Claims 16-19 depend from claim 13 and are allowable at least by virtue of that dependency. Accordingly, the rejection of these claims should be withdrawn.

Claim 20

Claim 20 recites a method for a second (base) computing device to authenticate content data made available by a first (mobile) computing device. The method includes steps of: (1) "accessing authentication information made available by the first computing device, the authentication information including the content data, a public key of the first computing device, a first network address of the first computing device, and a digital signature" (2) "deriving a portion of a second network address from the public key of the first computing device; (3) "validating the digital signature by using the public key of the first computing device;" and (4) "accepting the content data if the derived portion of the second network address matches a corresponding portion of the first network address and if the validating shows that the digital signature was generated from data in the set: the content data, a hash value of data including the content data."

Diffie does not disclose a base computing unit that receives a first network address of a mobile device that it subsequently decrypts with a public key of the mobile device to derive a second network address. Claim 20 recites a method having these particular steps so that the base computing device can unilaterally verify a valid network address for the mobile computing device.

Since Diffie does not disclose or anticipate each and every element recited in claim 20, claim 20 is allowable over Diffie and the rejection of claim 20 should be withdrawn.

Claims 21-24

Claims 21-24 depend from claim 20 and are allowable at least by virtue of that dependency. Accordingly, the rejection of these claims should be withdrawn.

Claim 25

Claims 25 recites a computer-readable media having instructions for implementing steps of: (1) "accessing authentication information made available by the first computing device, the authentication information including the content data, a public key of the first computing device, a first network address of the first computing device, and a digital signature" (2) "deriving a portion of a second network address from the public key of the first computing device" (3) "validating the digital signature by using the public key of the first computing device" and (4) "accepting the content data if the derived portion of the second network address matches a corresponding portion of the first network address and if the validating shows that the digital signature was generated from data in the set: the content data, a hash value of data including the content data."

As previously discussed, Diffie does not disclose or anticipate a vase computing device that receives authentication information from a mobile computing device that includes a first network address that can be decrypted with a public key of the mobile computing device to derive a second network address..

Accordingly, claim 25 is allowable over the cited reference and the rejection should be withdrawn.

CONCLUSION

In view of the foregoing remarks, this application should now be in condition for allowance. A notice to this effect is respectfully requested. If the Examiner believes, after this response, that the application is not in condition for allowance, the Examiner is encouraged to call the Applicant's attorney at the telephone number listed below.

If this response is not considered timely filed and if a request for an extension of time is otherwise absent, Applicant hereby requests any necessary extension of time. If there is a fee occasioned by this response, including an extension fee, please charge any deficiency to **Deposit Account No. 50-0463.**

Respectfully submitted,

MICROSOFT CORPORATION

Date: 6-8-05

By: _____
James R. Banowsky, Reg. No. 37,773
Microsoft Corporation
One Microsoft Way
Redmond, Washington 98052-6399
Telephone (425) 705-3539

CERTIFICATE OF MAILING OR TRANSMISSION			
I hereby certify that this correspondence is being deposited with the United States Postal Service with sufficient postage as first class mail in an envelope addressed to: Mail Stop RCE, Commissioner for Patents, P. O. Box 1450, Alexandria, VA 22313-1450 or facsimile transmitted to the U.S. Patent and Trademark Office on the date shown below.			
Signature			
Name	**Rimma N. Oks**	Date	**June 8, 2005**